Client (Personal) Certificates: Should We Be Thinking About Certificate Use Cases *or* Should We Be Thinking About The Sort of Credential Deployment Model We Need?

AMSAC Open Meeting, Internet2 Member Meeting
10/4/2011 4:30PM 306A

Joe St Sauver, Ph.D. (joe@internet2.edu or joe@uoregon.edu)
InCommon Certificate Program Manager and
Internet2 Nationwide Security Programs Manager

http://pages.uoregon.edu/joe/cases-or-creds/

The InCommon Certificate Service Has a Terrific New Capability: Client Certs

- In addition to having ready access to SSL web server certs, InCommon Certificate Service subscriber sites can now issue client certificates to their users. These certs may be referred to by many different names, including “personal certs,” “X.509 certs,” “PKI certs” etc.)

- Traditionally, client cert have been most strongly associated with signing and encrypting email with S/MIME.

- However, client certs can potentially also be used for other purposes, including document signing, user authentication and access control.

The Hard-To-Resist Temptation

- Given that flexibility, there's a hard-to-resist temptation, given this (or any) new capability, and that is to focus on how the new capability might be used:

  What are the use cases?
  What can we *do* with these new "client cert" things?

- I'm as guilty of that as anyone. If you give a kid a hatchet, they're going to want to go see what they can chop with it.

- Unfortunately, that may be a mistake -- let me tell you why.

Not All "Client Certs" Are The Same

- To keep this simple, let's just imagine two different types:

-- Model A: Lower Security

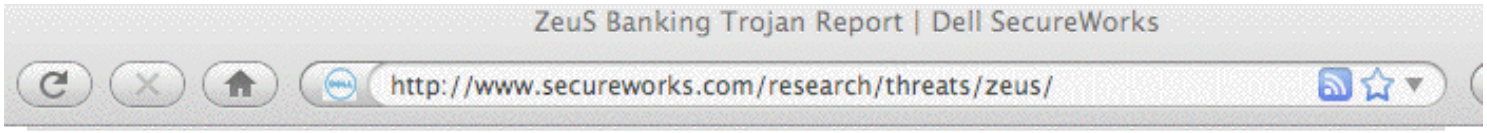
-- *Ad hoc* deployment: some users try them, most users don't
-- Requested/issued via the web with just an email confirmation
-- Stored on the user's system (and/or within applications)
-- Can be accessed/exported/copied/exfiltrated
-- May not require that a PIN/password be entered for cert use

-- Model B: Higher Security

-- Ubiquitous deployment using a standardized format
-- Issued face-to-face (and only after verifying the user's identity)
-- Key pairs get generated on smart cards (non-exportably)
-- Access to the cert requires password entry, and brute force password guessing attack attempts may lock access

(Some) Weaknesses of Model A

- If deployment is *ad hoc*, I can't count on *ALL* my users being able to use client certs -- I always need a "solution" for the exceptions
- I *think* I know who's obtained that cert (at least I know it was obtained by someone who had access to that *email address*)
- Because the certs are stored in the OS (and/or in application cert stores) in Model A, the cert may be duplicated by the user, and may also be potentially subject to being "harvested" by malware
- In Model A, access to certs may not require entry of a password. When that's true, if you use certs as a replacement for password access, paradoxically you may not end up with two factor authentication: one factor (a traditional pasword) may just end up being REPLACED by a *different* single factor (a password-less client cert).
- Password-less Model A certs may also have privacy implications: when you touch any site on the web, it could potentially ask for your client cert (& email address!) and you might not even know it



ZeuS Banking Trojan Report

- **Date:** March 11, 2010
- **Author:** Kevin Stevens and Don Jackson, Security Researchers
  SecureWorks Counter Threat Unit SM (CTU)

Introduction

This Threat Analysis from the SecureWorks CTU SM provides a brief overview of the current version of ZeuS and its modules, along with the market pricing. We will then see how ZeuS is actively being used and the irony of how the criminals themselves can sometimes be the victims.

ZeuS is a well-known banking Trojan horse program, also known as crimeware. This trojan steals data from infected computers via web browsers and protected storage. Once infected, the computer sends the stolen data to a bot command and control (C&C) server, where the data is stored.

ZeuS is sold in the criminal underground as a kit for around $3000-4000, and is likely the one malware most utilized by criminals specializing in financial fraud. ZeuS has evolved over time and includes a full arsenal of information stealing capabilities:

- Steals data submitted in HTTP forms
- Steals account credentials stored in the Windows Protected Storage
- Steals client-side X.509 public key infrastructure (PKI) certificates
- Steals FTP and POP account credentials
- Steals/deletes HTTP and Flash cookies
- Modifies the HTML pages of target websites for information stealing purposes

An Example of Model B: The Feds & HSPD-12

- We've already seen model B deployed: it's what the federal government has chosen to do for its HSPD-12 "CAC"/"PIV" card program, the ID cards now used by virtually all federal employees and contractors – they all have smart card "badges," badges which include a client cert as well as their name, their picture, bar codes, a mag stripe, etc.
- If you're a government employee (I'm not), reportedly you may end up using your CAC/PIV card *ALL* the time:

  -- When you come into your building, you do so with your card

  -- You (obviously) use it as a name badge

  -- You login to your workstation or the network with your card

  -- When you send email, it's signed or encrypted with your card

  -- When you access internal web sites, that access is gated by your card

One Point I Want To Stress

- Regardless of whether you decide you want to do Model A or Model B, higher education's client certificate program **isn't** run by the federal government and never **will be** run by the federal government. They don't want to take on that role, and we wouldn't want them to do so.

- I mentioned the feds on the previous slide simply because they have one of the largest deployment of client certificates.

- Lots of NON-governmental entities ALSO have client certificate deployments, including corporate household names like Boeing and HP. Note that when major corporations deploy client certs, with only rare exceptions, they virtually always do it "Model B" style.

Both Models Use Certificates, But Those ARE Two Radically Different Animals

- The casual, lower security model, Model A, isn't really very revolutionary. If you just want to know how to get started with Model A, see my "leveraging certs" talk from Tuesday 1:15PM

- Or, you might not need certs at all…

  -- You already can use PGP to sign and encrypt your email
  -- You can use ssh with private keys if you just want cryptographic key-based authentication for remote access
  -- If you're not fussy, and you just want *some* kind of 2nd factor auth, you could do one time passwords, or you could do 2nd channel auth via smart phones, or you could use biometrics, etc.

But Let's Think A Little More About Model B…

- Its almost certainly more secure:

  -- You've got one credential that "does it all" (with one password!)
  -- You always know who you're dealing with, so trust is enhanced
  -- More network traffic can potentially get transparently encrypted
  -- Phishing becomes impossible
  -- Need to disable access? Revoke the user's credential

- On the other hand:

  -- Anonymity largely disappears
  -- User privacy changes (but not always necessarily for the worse – remember, encryption becomes more ubiquitous)
  -- Things definitely FEEL different (the age of innocence is over?)
  -- Smart cards aren't free

So That's The Point I Ask You to Ponder Today…

- **What future would AMSAC like to see for the community? Model A? Model B? Both? Neither? Ask again in six months?**

- If we do take a cue from the feds, or Boeing, or HP, and try to encourage higher ed folks to do model B, should we:

  -- (a) encourage Internet2 sites to join the InCommon Certificate Service and (b) do client certs for their users?
  -- try to standardize on a single common physical card format?
  -- strive to negotiate lowest possible pricing for smart cards from commercial smart card vendors?
  -- other?

- Thanks for the chance to visit with you a little today!